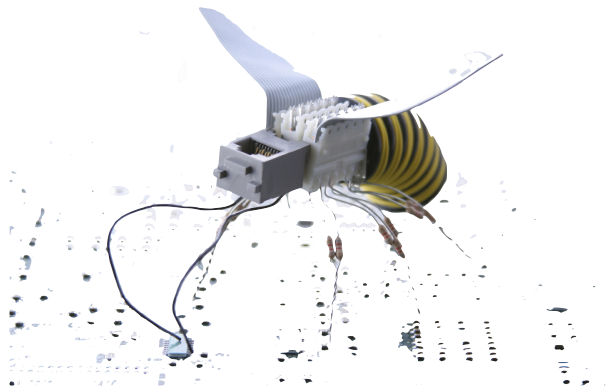




Technical Surveillance Countermeasures
Counter-Espionage Consulting

Client Briefing



CYBER ESPIONAGE

How exposed are you?

November 2009



Cyber Crime...

A Rapidly Growing Security Threat

A whole realm of new security threats have emerged as the result of advances in network and communications technology. Cybersecurity involves the protection, monitoring and authentication of communications or online information against unauthorised access, use, modification and theft. However, the borderless and transient nature of the internet now allows criminal elements greater access to legal and illegal markets, money laundering, digital funds and the ability to circumvent both national and international laws and censors. There are an endless number of risks relating to cybersecurity and these include viruses that can erase entire computer systems, unauthorised access to alter company files, mobile phone hacking, keystroke logging, damage to network infrastructures and the theft of financial or sensitive information.

Online Security

The threats to cybersecurity have been accentuated by the Global Financial Crisis and the huge black market for bank card and account information. There has been a dramatic increase in the number of phishing emails seeking personal banking information over the past year. Although email systems have traditionally been the primary method for distributing malware, other major attack vectors have become very common, including social networking sites, infected webpages and fake antivirus software.

There has been an exponential rise in the proliferation of malware and botnets spread through the internet. One recent study by Google found over that one in ten internet websites hosted code that could launch drive-by downloads of malicious programs or suspicious software. Over two-thirds of these malicious programs were capable of infecting computers with bot software that allowed data on banking transactions to be collected and emailed to a temporary email account. Meanwhile, a study by Panda Security recently found that there has been a six-fold increase since 2008 in the number computers being infected with malware engineered to steal personal information.

Malware, botnets, trojan worms and fake antivirus programs have become increasingly sophisticated and hard to detect. Botnets disrupt computer systems, block internet traffic, harvest information and distribute spam, viruses and other malicious code. They can allow a vast number of computers to be controlled remotely through commands sent via the internet. Botnets are becoming increasingly sophisticated and less centralised, making them more difficult to trace and counter. In April, security agencies disclosed information concerning one of the largest botnets discovered yet. It was revealed that 1.9 million computers had been infected with malicious software that allowed a Ukraine-based gang to read emails, copy files, record keystrokes and make screenshots. Access to the compromised computers was subsequently being sold on the black market in Russia.



The Homeland Security Department in the United States has stated that the number of cyber attacks on government civilian computer networks tripled between 2006 and 2008. Other governments worldwide have warned businesses to protect themselves against the threat posed by cyber attacks originating from China, with Chinese hackers allegedly compromising the computer systems of a number of government agencies and a range of companies worldwide. Australian Prime Minister Kevin Rudd's communications and computer usage were allegedly monitored during a visit to China in August 2008.

The recognition of the cyber threat was clearly shown by the 2009 Defence White Paper which placed cybersecurity on the same strategic level of importance as Australia's more traditional defence areas, reflecting the new priorities in global security.

Mobile Phone Espionage

There has recently been a great increase in the levels of telephone network hacking and mobile phone espionage. Mobile phone spy software is now widely available and very affordable, and the majority of mobile phones can quickly be modified or replaced, to become portable espionage tools. This security threat has increased as more mobile phones offer increased functionality, such as internet access. Generally speaking, the more complicated a phone is, the more easily it can be tapped. Spy software can be quickly downloaded onto a mobile phone within a few minutes, and such software can enable the phone's conversations to be listened to, text messages to be viewed, and the precise location of the phone to be pinpointed to within two to three metres using triangulation from telephone masts or base stations. Phone microphones can subsequently be switched on remotely, allowing conversations to be overheard even when the phone is not being used or in some cases, is switched off!

Precautions should be taken to reduce the risk of mobile phone espionage. Security passwords should be installed on all mobile phones and personnel should keep their phone within sight at all times to prevent the opportunity for spy software to be installed. Removing a phone's battery when not in use can be an effective security measure, however this is not always failsafe.

All organisations should invest in security measures to ensure that the mobile phones of high-level employees are kept secure, to prevent unnoticed espionage occurring. If there are any concerns that a mobile phone has been bugged, a replacement should be purchased immediately. The same process should apply if you are not sure whether the phone may have been previously sabotaged.



What Should Companies Do?

The law enforcement of cyber crime has become increasingly difficult as new technologies outpace policy and coordination among national and international agencies and corporations. Furthermore, the majority of cyber crime originates from unstable or corrupt countries, making law enforcement particularly difficult for international organisations and developed governments. As such, companies should invest in cybersecurity measures, particularly during these tough economic times, as both the private and governmental sectors become more susceptible to data theft and cyberattacks.

It is imperative that all organisations take their own precautions to minimise cyber security threats in order to avoid excess monetary losses, data theft, damage to infrastructure and liability issues that can result from the loss of sensitive personal information.

All organisations should have robust information security systems in place to protect sensitive information and guard against unauthorised access, as data breaches can cause great financial damage to organisations. A Ponemon Institute study earlier this year found that the average cost of a data breach to a company stood at US \$6.6 million (AUD \$7.2 million). As well as the financial implications, data breaches cause massive reputational damage to organisations.

Cyber security entails a battle of technology. Traditional security measures are no longer adequate to guard against the borderless threats posed by the internet and transnational criminal groups. Security systems constantly need to be upgraded to match the technological advances being made and utilised by cyber criminals. Although firewalls offer a certain level of protection, they offer very limited protection against viruses that spread through the running of infected programs.

Organisations can take a number of simple steps to help improve their own cybersecurity:

- ▶ Effective anti-virus software should be installed and regularly upgraded on all company computers.
- ▶ Legitimate anti-spyware programs should be frequently run (if not incorporated in the anti-virus software already being utilised) to scan computer networks and remove any spyware or adware hidden in programs.
- ▶ All data should be regularly backed up to reduce the negative consequences that can result from lost or altered files, and sensitive files should be encrypted to ensure that unauthorised viewing cannot occur, even when physical access is possible. Confidential files should be adequately erased, not merely 'deleted', once they are no longer needed.
- ▶ Access passwords should be carefully chosen, regularly changed and not written down to minimise unauthorised access to computer networks.



The vast majority of data breaches can generally be traced back to insider negligence or fraud.

Since the financial crisis has led to high levels of redundancies, disillusioned workers and economic inequality, such internal risks are currently heightened.

A positive workplace cybersecurity culture should be established along with a whistle blowing system, through which suspicious employee behaviour can be anonymously reported. Employees should be educated about up-to-date cybersecurity practices.

Huge volumes of information can be transferred and stolen in a few seconds using personal emails or portable USB drives. As such, a no-USB drive policy should be established and personal email accounts should be blocked on work computers. Companies should closely regulate and monitor the downloading and transfer of all confidential or commercially-sensitive information.

Computers should be logged off whenever they are left unattended, and companies should establish a practise whereby computers are automatically logged off after a set period of inactivity. In a similar vein, computers should be disconnected from the internet when not in use, if they contain highly-sensitive data.



How We Can Assist

Cyber security requires strong intelligence and an increased awareness of potential vulnerabilities. Jayde Consulting works with a range of organisations to ensure appropriate controls and measures are in place to reduce the risks associated with cyber crime. Jayde's highly specialised operatives utilise the most up-to-date technical surveillance counter measures techniques in order to help detect whether espionage is occurring.

A proactive approach to security will assist in protecting your privacy, property and reputation.

All advice, services and consulting offered is on a strictly confidential basis. Our clients return to us, because they know that we will not discuss their cases with anyone. No exceptions. Integrity is paramount.

For further information on our counter-espionage services, please contact us via:

Website www.jaydeconsulting.com

Email contactus@jaydeconsulting.com

Telephone +61 [0] 2 8006 0635